On Reversible Cellular Automata with Triplet Local Rules

Shuichi INOKUCHI*, Kazumasa HONDA†, Hyen Yeal LEE‡, Tatsuro SATO§, Yoshihiro MIZOGUCHI* and Yasuo KAWAHARA†

Abstract

Bijections between sets may be seen as discrete (or crisp) unitary transformations used in quantum computations. So discrete quantum cellular automata are cellular automata with reversible transition functions. This note studies on 1d reversible cellular automata with triplet local rules.

1 Introduction

Since Feynman proposed the notion of "quantum computation", a lot of models of quantum computation have been investigated. Watrous[4] introduces the notion of quantum cellular automata(QCA, for short) of a kind of quantum computer and showed that any quantum Turing machines can be simulated by a partitioned QCA(PQCA) with constant slowdown. Moreover he presented necessary and sufficient conditions for the well-formedness of 1d PQCA. Watrous' QCA have infinite cell arrays. Inokuchi and Mizoguchi[9] introduced a notion of cyclic QCA with finite cell array, which generalises PQCA, and formulated sufficient condition for local transition functions to form QCA. Quantum computations are performed by means of applying unitary transformations for quantum states. So classical cellular automata(CA) with reversible transition functions are considered as a special type of QCA.

On the other hand CA have also been studied as models of universal computation and complex systems [1, 3, 5, 6]. Reversible CA and the reversibility of CA were discussed by many researchers. Wolfram[8] investigated the reversibility of several models of CA and showed that only six CA, whose transition functions are identity function, right-shift function, left-shift function and these complement functions, of the 256 elementary CA with infinite cell array are reversible. Dow[7] investigated the injectivity(reversibility) of additive CA with finite cyclic cell array and infinite cell array, and showed the relation between

*Faculty of Mathematics, Kyushu University 33, Fukuoka 812-8581, Japan.
†Department of Informatics, Kyushu University 33, Fukuoka 812-8581, Japan.
‡School of Computer Engineering, Pusan National University, Pusan 609-735, Korea.
§Oita National College of Technology, Oita, 870-0152, Japan.

injectivities of these additive CA. Morita and Harao[2] showed that for any reversible Turing machine there is a reversible CA that simulates it.

This paper treats with 1d CA, denoted by $CA-R(n)$, with finite cell array, triplet local rule of rule number R and two states, and investigate the reversibility of $CA-R(n)$. We can easily observe dynamical behaviors of $CA-R(n)$ by computer simulations, and consequently get the following table which shows whether 1d cellular automata $CA-R(n)$ are reversible or not, according to five types of boundary conditions a-b, a-$*$, $*$-b, $*$-$*$ and $*$, which will be defined in the next section.

Rule numbers	a-b	a-$*$	$*$-b	$*$-$*$	$*$
51, 204	○	○	○	○	○
15, 85, 170, 240					○
90, 165	○	○	○		
60,195	○	○			
102,153	○		○		
150,105	○	○	○	○	○
166,180,154,210,89,75,101,45					○

Although for 1d CA with infinite cell array there exist only six trivial reversible CA, we will prove that there exist several non trivial reversible 1d CA with finite cell array.

2 Cellular Automata $CA-R$

Cellular automata treated in the paper have linearly ordered and finite number cells bearing with states 0 or 1. The next state of any cell depends upon the states of left cell, the cell itself and the right cell. In this section we will formally define cellular automata $CA-R(n)$ with rule number R of triplet local rule and n cell array.

Let Q be a state set $\{0,1\}$ and n a positive integer. The complement of a state $a \in Q$ will be denoted by a^-, that is, $a^- = 1-a$. The state set Q forms an additive group by the addition $+$ (modulo 2) (the exclusive logical sum), that is, $0+0=1+1=0$ and $0+1=1+0=1$. Remark that $a^- = 1+a$ for all states $a \in Q$. The n-th cartesian product of Q is denoted by Q^n, in other words, Q^n is the set of all n-tuples consisting of 0 and 1. For example,

$$Q^3 = \{000, 001, 010, 011, 100, 101, 110, 111\}.$$

An n-tuple $x = x_1x_2\cdots x_n \in Q^n$ may be called a word of length n over Q, or a configuration in a context of cellular automata. It is obvious that the n-th cartesian product Q^n also forms an additive group by the component-wise addition, that is,

$$x_1x_2\cdots x_n + y_1y_2\cdots y_n = (x_1+y_1)(x_2+y_2)\cdots(x_n+y_n)$$

for all n-tuples $x_1x_2\cdots x_n, y_1y_2\cdots y_n \in Q^n$.

A *triplet local (transition) rule* is a function $f : Q^3 \to Q$ and the *rule number* $|f|$ of f is defined by

$$|f| \quad = \quad \sum_{a,b,c\in Q} 2^{4a+2b+c} f(abc).$$

Note that the rule number $|f|$ is a natural number with $0 \le |f| \le 255$. A triplet local rule with rule number R will be denoted by f_R, namely $|f_R| = R$.

Let $f : Q^3 \to Q$ be a triplet local rule. The *symmetric rule* $f^\sharp : Q^3 \to Q$ of f is defined by

$$f^\sharp(abc) = f(cba)$$

for all triples $abc \in Q^3$. It is trivial that $f^{\sharp\sharp} = f$ and

$$|f^\sharp| = |f| + 56(r_3 - r_6) + 14(r_1 - r_4)$$

where $r_{4a+2b+c} = f(abc)$ for all triples $abc \in Q^3$. The *complementary rule* $f^- : Q^3 \to Q$ of f is defined by

$$f^-(abc) = [f(abc)]^-$$

for all triples $abc \in Q^3$. Note that $f^{--} = f$ and $f^{-\,\sharp} = f^{\sharp\,-}$ and

$$|f^-| = 255 - |f|.$$

The *reverse rule* $f^\circ : Q^3 \to Q$ of f is defined by

$$f^\circ(abc) = [f(a^-b^-c^-)]^-$$

for all triples $abc \in Q^3$. It is trivial that $f^{\circ\circ} = f$, $f^{\sharp\circ} = f^{\circ\sharp}$ and

$$|f^\circ| = 255 - (128r_0 + 64r_1 + 32r_2 + 16r_3 + 8r_4 + 4r_5 + 2r_6 + r_7).$$

A *dynamical system* is a pair (X, δ) of a set X and a transition function $\delta : X \to X$.

Let $f : Q^3 \to Q$ be a triplet local rule, n a positive integer and $a, b \in Q$. By setting different boundary conditions we can define five transition functions $f_{(n),a-b} : Q^n \to Q^n$, $f_{(n),*} : Q^n \to Q^n$, $f_{(n),*-*} : Q^n \to Q^n$, $f_{(n),a-*} : Q^n \to Q^n$ and $f_{(n),*-b} : Q^n \to Q^n$ as follows.

$$f_{(n),a-b}(x_1x_2\cdots x_{n-1}x_n) = f(a\,x_1x_2)f(x_1x_2x_3)\cdots f(x_{n-2}x_{n-1}x_n)f(x_{n-1}x_nb),$$

$$f_{(n),*}(x_1x_2\cdots x_{n-1}x_n) = f(x_nx_1x_2)f(x_1x_2x_3)\cdots f(x_{n-2}x_{n-1}x_n)f(x_{n-1}x_nx_1),$$

$$f_{(n),*-*}(x_1x_2\cdots x_{n-1}x_n) = f(x_1x_1x_2)f(x_1x_2x_3)\cdots f(x_{n-2}x_{n-1}x_n)f(x_{n-1}x_nx_n),$$

$$f_{(n),a-*}(x_1x_2\cdots x_{n-1}x_n) = f(a\,x_1x_2)f(x_1x_2x_3)\cdots f(x_{n-2}x_{n-1}x_n)f(x_{n-1}x_nx_n),$$

$$f_{(n),*-b}(x_1x_2\cdots x_{n-1}x_n) = f(x_1x_1x_2)f(x_1x_2x_3)\cdots f(x_{n-2}x_{n-1}x_n)f(x_{n-1}x_nb)$$

for all n-tuples $x_1x_2\cdots x_{n-1}x_n \in Q^n$ and all states $a, b \in Q$.

Set rule number $R = |f|$ $(0 \leq R \leq 255)$. Cellular automata $CA{-}R_{a-b}(n)$ with fixed boundary $a{-}b$, $CA{-}R_*(n)$ with cyclic boundary, $CA{-}R_{*-*}(n)$ with free boundary, $CA{-}R_{a-*}(n)$ with right free boundary $a{-}*$ and $CA{-}R_{*-b}(n)$ with left free boundary $*{-}b$ are dynamical systems $(Q^n, f_{(n),a-b})$, $(Q^n, f_{(n),*})$, $(Q^n, f_{(n),*-*})$, $(Q^n, f_{(n),a-*})$ and $(Q^n, f_{(n),*-b})$, respectively. This is denoted by the followings for short;

$$CA{-}|f|_{\{a-b,a-*,*-b,*-*,*\}}(n) = (Q^n, f_{(n),\{a-b,a-*,*-b,*-*,*\}}).$$

Transition functions $\delta : Q^n \to Q^n$ are not always bijections, but when it is the case we can regard them as discrete quantum automata.

Definition 2.1 (a) A triplet local rule $f : Q^3 \to Q$ is *additive* if $f(abc + a'b'c') = f(abc) + f(a'b'c')$ for all triples $abc, a'b'c' \in Q^3$.

(b) A transition function $\delta : Q^n \to Q^n$ is *additive* if $\delta(x + x') = \delta(x) + \delta(x')$ for all configurations $x, x' \in Q^n$.

We now recall the basic fact on the reversibility of dynamical systems over Q^n.

Lemma 2.2 (a) *A transition function $\delta : Q^n \to Q^n$ is bijective iff it is injective iff it is surjective.*

(b) *If a triplet local rule $f : Q^3 \to Q$ is additive, then so is the transition function $f_{(n),\{0-0,0-*,*-0,*-*.*\}} : Q^n \to Q^n$ for all positive integers n.*

(c) *An additive transition function $\delta : Q^n \to Q^n$ is bijective iff $\delta(x) = 0^n$ implies $x = 0^n$ for all configurations $x \in Q^n$.*

Proof. (1) It is trivial since the set Q^n is finite. Also (2) and (3) are clear. $\square$

3 Basic Results

In this section we show some general properties of cellular automata $CA{-}R(n)$. Let (X, δ) and (Y, γ) be two dynamical systems. An *isomorphism* $t : (X, \delta) \to (Y, \gamma)$ is a bijection $t : X \to Y$ rendering the following square commutative:

$$\begin{tikzcd} X \arrow[r, "t"] \arrow[d, "\delta"'] & Y \arrow[d, "\gamma"] \\ X \arrow[r, "t"'] & Y. \end{tikzcd}$$

We call (X, δ) and (Y, γ) isomorphic, denoted by $(X, \delta) \cong (Y, \gamma)$, if there exists an isomorphism between (X, δ) and (Y, γ). It is trivial that isomorphic dynamical systems are essentially the same ones.

Lemma 3.1 *The followings holds;*

(a) $CA{-}|f^\sharp|_{\{a-b,a-*,*-b,*-*,*\}}(n) \cong CA{-}|f|_{\{b-a,*-a,b-*,*-*,*\}}(n)$.

(b) $CA{-}|f^\circ|_{\{a-b,a-*,*-b,*-*,*\}}(n) \cong CA{-}|f|_{\{a^- -b^-,a^- -*,*-b^-,*-*,*\}}(n)$.

Proof.

(a) This fact asserts the following five statements:

(a) $CA{-}|f^\sharp|_{a-b}(n) \cong CA{-}|f|_{b-a}(n)$,
(b) $CA{-}|f^\sharp|_{a-*}(n) \cong CA{-}|f|_{*-a}(n)$,
(c) $CA{-}|f^\sharp|_{*-b}(n) \cong CA{-}|f|_{b-*}(n)$,
(d) $CA{-}|f^\sharp|_{*-*}(n) \cong CA{-}|f|_{*-*}(n)$,
(e) $CA{-}|f^\sharp|_{*}(n) \cong CA{-}|f|_{*}(n)$.

It is easy to show that a bijection $t_n : Q^n \to Q^n$ defined by $t_n(x_1 x_2 \cdots x_n) = x_n \cdots x_2 x_1$ gives an isomorphism. We will prove only $t_n \circ f_{(n),a-b} = f^\sharp_{(n),b-a} \circ t_n$.

$$\begin{aligned}
(t_n \circ f_{(n),a-b})(x_1 x_2 \cdots x_n) &= t_n(f(ax_1x_2)f(x_1x_2x_3)\cdots f(x_{n-1}x_nb)) \\
&= f(x_{n-1}x_nb)\cdots f(x_1x_2x_3)f(ax_1x_2) \\
&= f^\sharp(bx_nx_{n-1})\cdots f^\sharp(x_3x_2x_1)f^\sharp(x_2x_1a) \\
&= f^\sharp_{(n),b-a}(x_n \cdots x_2 x_1) \\
&= (f^\sharp_{(n),b-a} \circ t_n)(x_1 x_2 \cdots x_n).
\end{aligned}$$

(b) This can be shown in the same way as a.

□

Corollary 3.2

$$\begin{aligned}
CA{-}|f|_{\{a-b,a-*,*-b,*-*,*\}}(n) &\cong CA{-}|f^\sharp|_{\{b-a,*-a,b-*,*-*,*\}}(n) \\
&\cong CA{-}|f^\circ|_{\{a^- -b^-,a^- -*,*-b^-,*-*,*\}}(n) \\
&\cong CA{-}|f^{\sharp\circ}|_{\{b^- -a^-,*-a^-,b^- -*,*-*,*\}}(n).
\end{aligned}$$

Thus a quartet $[|f|,|f^\sharp|,|f^\circ|,|f^{\sharp\circ}|]$ of rule numbers $|f|$, $|f^\sharp|$, $|f^\circ|$ and $|f^{\sharp\circ}|$ is an equivalence class of rule numbers which represent isomorphic triplet local rules. For example, $[102, 60, 153, 195]$ and $[89, 75, 101, 45]$.

Lemma 3.3
$CA{-}|f^-|_{\{a-b,a-*,*-b,*-*,*\}}(n)$ is reversible iff so is $CA{-}|f|_{\{a-b,a-*,*-b,*-*,*\}}(n)$.

Proof. It simply follows from

$$f^-_{(n),\{a-b,a-*,*-b,*-*,*\}} = c_n \circ f_{(n),\{a-b,a-*,*-b,*-*,*\}},$$

where $c_n : Q^n \to Q^n$ is a bijection defined by $c_n(x_1x_2\cdots x_n) = x_1^- x_2^- \cdots x_n^-$. We will prove only $f^-_{(n),a-b} = c_n \circ f_{(n),a-b}$.

$$\begin{aligned} f^-_{(n),a-b}(x_1x_2\cdots x_n) &= f^-(ax_1x_2)f^-(x_1x_2x_3)\cdots f^-(x_{n-1}x_nb) \\ &= c_n(f(ax_1x_2)f(x_1x_2x_3)\cdots f(x_{n-1}x_nb)) \\ &= (c_n \circ f_{(n),a-b})(x_1x_2\cdots x_n). \end{aligned}$$

□

Lemma 3.4 *Let k and n be positive integers. If $CA{-}|f|_*(kn)$ is reversible, then so is $CA{-}|f|_*(n)$.*

Proof. We will see that the injectivity of $f_{(kn),*} : Q^{kn} \to Q^{kn}$ implies that of $f_{(n),*} : Q^n \to Q^n$. The result easily follows from a fact that the identity

$$\begin{aligned} & f_{(kn),*}(x_1x_2\cdots x_nx_1x_2\cdots x_n\cdots x_1x_2\cdots x_n) \\ = \; & f_{(n),*}(x_1x_2\cdots x_n)f_{(n),*}(x_1x_2\cdots x_n)\cdots f_{(n),*}(x_1x_2\cdots x_n) \end{aligned}$$

$$f_{(kn),*}(x^k) = (f_{(n),*}(x))^k$$

holds for all $x = x_1x_2\cdots x_n \in Q^n$. □

Lemma 3.5 *Let k and n be positive integers. If $CA{-}|f|_{*-*}((2k+1)n)$ is reversible, then so is $CA{-}|f|_{*-*}(n)$.*

Proof. The result easily follows from a fact that the identity

$$\begin{aligned} & f_{((2k+1)n),*-*}((x_1x_2\cdots x_nx_nx_{n-1}\cdots x_1)^k x_1x_2\cdots x_n) \\ = \; & (f_{(n),*-*}(x_1x_2\cdots x_n)f_{(n),*-*}(x_nx_{n-1}\cdots x_1))^k f_{(n),*-*}(x_1x_2\cdots x_n) \end{aligned}$$

holds for all $x_1x_2\cdots x_n \in Q^n$. □

4 $CA{-}\{204, 51\}(n)$

Triplet local rules $f_{\{204,51\}} : Q^3 \to Q$ are given, defined by $f_{204}(abc) = b$ and $f_{51}(abc) = b^-$ for all triples $abc \in Q^3$. So it holds that $f^-_{204} = f_{51}$, $[204, 204, 204, 204]$ and $[51, 51, 51, 51]$. Hence equalities

$$f_{204(n),\{a-b,a-*,*-b,*-*,*\}} = \mathrm{id}_{Q^n} \quad \text{and} \quad f_{51(n),\{a-b,a-*,*-b,*-*,*\}} = c_n$$

hold. Thus all configurations in $CA{-}204(n)$ are fixed points, i.e. $CA{-}204(n) \cong 2^n\langle 1\rangle$, and all configurations in $CA - 51(n)$ lie on limit cycles of period 2, i.e. $CA - 51(n) \cong 2^{n-1}\langle 2\rangle$ where $\langle n\rangle$ denotes a limit cycle of period n.

Corollary 4.1 $CA - \{204, 51\}_{\{a-b,a-*,*-b,*-*,*\}}(n)$ *are reversible for all positive integers n.*

5 $CA\text{–}\{240, 170, 15, 85\}(n)$

Since $f_{240}(abc) = a$, $f_{170}(abc) = c$, $f_{15}(abc) = a^-$ and $f_{85}(abc) = c^-$ for all triples $abc \in Q^3$, we have $f_{240}^- = f_{15}$, $[240, 170, 240, 170]$ and $[15, 85, 15, 85]$. Thus it is trivial that $f_{\{240,170,15,85\}(n),*}$ are bijective for all positive integers n.

Corollary 5.1 *$CA\text{–}\{240, 170, 15, 85\}_*(n)$ are reversible for all positive integers n.*

Lemma 5.2 (a) $f_{15(n),\{a-b,a-*,*-b,*-*,*\}} = f_{240(n),\{a^- -b,a^- -*,*-b,*-*,*\}} \circ c_n$,

(b) $f_{85(n),\{a-b,a-*,*-b,*-*,*\}} = f_{170(n),\{a-b^-,a-*,*-b^-,*-*,*\}} \circ c_n$.

Proof. We will show only $f_{15(n),a-b} = f_{240(n),a^- -b} \circ c_n$.

$$\begin{aligned} f_{15(n),a-b}(x_1x_2\cdots x_n) &= f_{15}(ax_1x_2)f_{15}(x_1x_2x_3)\cdots f_{15}(x_{n-1}x_nb) \\ &= a^-x_1^-x_2^-\cdots x_{n-1}^- \\ &= f_{240}(a^-x_1^-x_2^-)f_{240}(x_1^-x_2^-x_3^-)\cdots f_{240}(x_{n-1}^-x_n^-b) \\ &= f_{240(n),a^- -b}(x_1^-x_2^-\cdots x_n^-) \\ &= (f_{240(n),a^- -b} \circ c_n)(x_1x_2\cdots x_n). \end{aligned}$$

$\square$ Remark. $(f_{240(n),*})^n = (f_{170(n),*})^n = \mathrm{id}_{Q^n}$ and $(f_{15(n),*})^n = (f_{85(n),*})^n = (c_n)^n$.

Lemma 5.3 *$CA - \{240, 170, 15, 85\}_{\{a-b,a-*,*-b,*-*\}}(n)$ are not reversible for all positive integers n.*

Proof. It simply follows from

$$f_{240(n),\{a-b,a-*,*-b,*-*\}}(a^n) = f_{240(n),\{a-b,a-*,*-b,*-*\}}(a^{n-1}a^-) = a^n.$$

$\square$

6 $CA\text{–}\{90, 165\}(n)$

It is obvious that $f_{90}(abc) = a + c$ and $f_{165}(abc) = (a + c)^-$ for all triples $abc \in Q^3$, and $[90, 90, 165, 165]$. Hence by Corollary 3.2 we have

$$CA\text{–}165_{\{a-b,a-*,*-b,*-*,*\}}(n) \cong CA\text{–}90_{\{a^- -b^-,a^- -*,*-b^-,*-*,*\}}(n)$$

and so we will inspect only $CA\text{–}90(n)$.

Lemma 6.1 *Let $x = x_1x_2\cdots x_n \in Q^n$. If $f_{90(n),\{a-b,a-*,*-b,*-*,*\}}(x) = 0^n$, then $x_i = x_{i+2}$ for all $i = 1, 2, \cdots, n-2$.*

Proof. Set $f = f_{90}$. The condition $f_{90(n),\{a-b,a-*,*-b,*-*,*\}}(x) = 0^n$ means

$$f(*\,x_1x_2)f(x_1x_2x_3)\cdots f(x_{n-2}x_{n-1}x_n)f(x_{n-1}x_n\,*) = 0^n.$$

Hence we have $x_i + x_{i+2} = f(x_ix_{i+1}x_{i+2}) = 0$ for all $i = 1, 2, \cdots, n-2$. $\square$

Lemma 6.2 (a) *$CA{-}90_{a-b}(n)$ is reversible iff so is $CA{-}90_{0-0}(n)$.*

(b) *$CA{-}90_{0-0}(n)$ is reversible iff $n = 0 \pmod 2$.*

Proof.

(a) It is immediate from a fact that $f_{90(n),a-b}(x) = f_{90(n),0-0}(x) + a0^{n-2}b$ for all $x \in Q^n$.

(b) First we will show that $f_{90(n),0-0}$ is injective for $n = 0 \pmod 2$, since $f_{90(n),0-0}$ is additive. (Cf. Lemma 2.2.)
(i) Set $f = f_{90}$. It holds that $f_{(2),0-0}(x_1x_2) = f(0x_1x_2)f(x_1x_20) = x_2x_1$. Hence $CA{-}90_{0-0}(2)$ is reversible.
(ii) Assume that $CA{-}90_{0-0}(n)$ is reversible for $n \geq 2$, i.e. $f_{(n),0-0}$ is injective. We will see that $f_{(n+2),0-0}$ is also injective.
Assume $f_{(n+2),0-0}(x_1x_2\cdots x_nx_{n+1}x_{n+2}) = 0^{n+2}$. Then we have

$$\begin{aligned} f_{(n),0-0}(x_1x_2\cdots x_n) &= f(0x_1x_2)f(x_1x_2x_3)\cdots f(x_{n-1}x_n0) \\ &= 0^{n-1}f(x_{n+1}x_{n+2}0) \\ &= 0^n, \end{aligned}$$

since $x_{n-1} = x_{n+1}$ and $x_n = x_{n+2}$ by Lemma 6.1. Hence by the induction hypothesis we have $x_1x_2\cdots x_n = 0^n$ and consequently $x_{n+1} = x_{n+2} = 0$. Therefore $CA{-}90_{0-0}(n+2)$ is reversible. Finally we see that if $n = 1 \pmod 2$ then $f_{90(n),0-0}$ is not injective. This follows at once from a fact that

$$f_{90(2k-1),0-0}((10)^{k-1}1) = 0^{2k-1}$$

holds for all positive integers k.

□

Corollary 6.3 *$CA{-}90_{a-b}(n)$ is reversible iff $n = 0 \pmod 2$.*

In the same discussion as Lemma 6.2 the following lemma can be shown.

Lemma 6.4 (a) *$CA{-}90_{a-*}(n)$ is reversible iff so is $CA{-}90_{0-*}(n)$.*

(b) *$CA{-}90_{0-*}(n)$ is reversible for all positive integers n.*

Corollary 6.5 *$CA{-}90_{\{a-*,*-b\}}(n)$ are reversible for all positive integers n.*

Lemma 6.6 *$CA{-}90_{\{*-*,*\}}(n)$ are not reversible for all positive integers n.*

Proof.
It directly follows from $f_{90(n),\{*-*,*\}}(1^n) = f_{90(n),\{*-*,*\}}(0^n) = 0^n$. □

7 $CA-\{102, 60, 153, 195\}(n)$

It is obvious that $f_{102}(abc) = b + c$, $f_{60}(abc) = a + b$, $f_{153}(abc) = (b + c)^-$, $f_{195}(abc) = (a + b)^-$ for all triples $abc \in Q^3$, and $[102, 60, 153, 195]$. Hence by Corollary 3.2 cellular automata $CA-\{60, 153, 195\}(n)$ are isomorphic to $CA-102(n)$ and so we will inspect only $CA-102(n)$.

Lemma 7.1 *Let $x = x_1x_2\cdots x_n \in Q^n$. If $f_{102(n),\{a-b,a-*,*-b,*-*,*\}}(x) = 0^n$, then $x_1 = x_2 = \cdots = x_{n-1} = x_n$.*

Proof. Set $f = f_{102}$. The condition $f_{(n),\{a-b,a-*,*-b,*-*,*\}}(x) = 0^n$ means that

$$f(*\,x_1x_2)f(x_1x_2x_3)\cdots f(x_{n-2}x_{n-1}x_n)f(x_{n-1}x_n\,*) = 0^n.$$

Hence we have $x_i + x_{i+1} = f(x_{i-1}x_ix_{i+1}) = 0$ for all $i = 1, 2, \cdots, n-1$. □

Lemma 7.2 (a) *$CA-102_{\{a-b,*-b\}}(n)$ is reversible iff so is $CA-102_{\{0-0,*-0\}}(n)$.*

(b) *$CA-102_{\{0-0,*-0\}}(n)$ are reversible for all positive integers n.*

Proof.

(a) It simply follows from a fact that $f_{102(n),\{a-b,*-b\}}(x) = f_{102(n),\{0-0,*-0\}}(x) + 0^{n-1}b$ holds.

(b) Set $f = f_{102}$. Since $f_{(n),\{0-0,*-0\}} : Q^n \to Q^n$ is additive (modulo 2), we will show that $f_{(n),\{0-0,*-0\}}(x) = 0^n$ implies $x = 0^n$ in $CA-102_{\{0-0,*-0\}}(n)$ for all positive integers n.

(i) It holds that $f_{(1),\{0-0,*-0\}}(x_1) = f(*x_10) = x_1$ and $f_{(2),\{0-0,*-0\}}(x_1x_2) = f(*x_1x_2)f(x_1x_20) = (x_1+x_2)x_2$. Hence $CA-102_{\{0-0,*-0\}}(n)$ is reversible for $n = 1, 2$.

(ii) Assume that $CA-102_{\{0-0,*-0\}}(n)$ for $n \geq 2$ is reversible, i.e. $f_{(n),\{0-0,*-0\}}(x_1\cdots x_n) = 0^n$ implies $x_1\cdots x_n = 0^n$. We now see that

$$f_{(n+1),\{0-0,*-0\}}(x_1\cdots x_nx_{n+1}) = 0^{n+1} \text{ implies } x_1\cdots x_nx_{n+1} = 0^{n+1}.$$

Assume $f_{(n+1),\{0-0,*-0\}}(x_1\cdots x_nx_{n+1}) = 0^{n+1}$. Then we have

$$\begin{aligned} f_{(n),\{0-0,*-0\}}(x_1\cdots x_n) &= f(*x_1x_2)f(x_1x_2x_3)\cdots f(x_{n-1}x_n0) \\ &= 0^{n-1}f(x_nx_{n+1}0) \\ &= 0^n, \end{aligned}$$

since $x_{n-1}x_n = x_nx_{n+1}$ by Lemma 7.1. Hence by the induction hypothesis we have $x_1\cdots x_n = 0^n$. Therefore $CA-102_{\{0-0,*-0\}}(n+1)$ is reversible.

□

Corollary 7.3 *$CA-102_{\{a-b,*-b\}}(n)$ are reversible for all positive integers n.*

Lemma 7.4 *$CA-102_{\{a-*,*-*,*\}}(n)$ are not reversible for all integers n.*

Proof. It is direct from $f_{102(n),\{a-*,*-*,*\}}(1^n) = f_{102(n),\{a-*,*-*,*\}}(0^n) = 0^n$. □

8 $CA{-}\{150,105\}(n)$

It is obvious that $f_{150}(abc) = a+b+c$, $f_{105}(abc) = (a+b+c)^-$ for all triples $abc \in Q^3$, $f_{150}^- = f_{105}$, $[150,150,150,150]$ and $[105,105,105,105]$. Hence by Lemma 3.3 the reversibility of $CA{-}105(n)$ and $CA{-}150(n)$ are equivalent and so we will inspect only $CA{-}150(n)$.

Lemma 8.1 *Let $x = x_1x_2\cdots x_n \in Q^n$. If $f_{150(n),\{a-b,a-*,*-b,*-*,*\}}(x) = 0^n$, then $x_i = x_{i+3}$ for all $i = 1,2,\cdots,n-3$.*

Proof. Set $f = f_{150}$. The condition $f_{(n),\{a-b,a-*,*-b,*-*,*\}}(x) = 0^n$ means

$$f(*\,x_1x_2)f(x_1x_2x_3)\cdots f(x_{n-2}x_{n-1}x_n)f(x_{n-1}x_n\,*) = 0^n.$$

Hence we have

$$x_i + x_{i+3} = f(x_ix_{i+1}x_{i+2}) + f(x_{i+1}x_{i+2}x_{i+3}) = 0+0 = 0$$

for all $i = 1,2,\cdots,n-3$. □

Corollary 8.2 *$CA{-}150_{\{*-*,*\}}(n)$ are reversible iff $n \not\equiv 0 \pmod 3$.*

Proof. Set $f = f_{150}$. First we will show that $f_{(n),\{*-*,*\}}(x) = 0^n$ implies $x = 0^n$ in $CA{-}150_*(n)$ for $n \not\equiv 0 \pmod 3$.
(i) It holds that $f_{(1),\{*-*,*\}}(x_1) = x_1$, $f_{(2),*-*}(x_1x_2) = x_2x_1$, $f_{(2),*}(x_1x_2) = x_1x_2$, $f_{(4),*-*}(x_1x_2x_3x_4) = x_2(x_1{+}x_2{+}x_3)(x_2{+}x_3{+}x_4)x_3$ and $(f_{(4),*})^2(x_1x_2x_3x_4) = x_1x_2x_3x_4$. Hence $CA{-}150_{\{*-*,*\}}(n)$ is reversible for $n = 1,2,4$.
(ii) Assume that $CA{-}150_{\{*-*,*\}}(n)$ is reversible for $n \ge 2$, i.e. $f_{(n),\{*-*,*\}}$ is injective. We will see that $f_{(n+3),\{*-*,*\}}$ is injective.
Assume $f_{(n+3),\{*-*,*\}}(x_1x_2\cdots x_nx_{n+1}x_{n+2}x_{n+3}) = 0^{n+3}$. Then we have

$$\begin{aligned} f_{(n),\{*-*,*\}}(x_1x_2\cdots x_n) &= f(\{x_1,x_n\}\,x_1x_2)f(x_1x_2x_3)\cdots f(x_{n-1}x_n\,\{x_n,x_1\}) \\ &= f(\{x_1,x_{n+3}\}\,x_1x_2)0^{n-2}f(x_{n+2}x_{n+3}\,\{x_{n+3},x_1\}) \\ &= 0^n, \end{aligned}$$

since $x_n = x_{n+3}$ and $x_{n-1} = x_{n+2}$ by Lemma 8.1. Hence by the induction hypothesis we have $x_1x_2\cdots x_n = 0^n$ and so $x_{n+1} = x_{n+2} = x_{n+3} = 0$. Finally we see that if $n \equiv 0 \pmod 3$ then $f_{150(n),\{*-*,*\}}$ is not injective. It follows at once from a fact that $f_{150(3k),\{*-*,*\}}((101)^k) = 0^{3k}$ holds for all positive integers k. □

Lemma 8.3 (a) *$CA{-}150_{a-b}(n)$ is reversible iff so is $CA{-}150_{0-0}(n)$.*

(b) *$CA{-}150_{a-*}(n)$ is reversible iff so is $CA{-}150_{0-*}(n)$.*

(c) *$CA{-}150_{0-0}(n)$ is reversible iff $n \not\equiv 2 \pmod 3$.*

(d) *$CA{-}150_{0-*}(n)$ is reversible iff $n \not\equiv 1 \pmod 3$.*

Proof. (1,2) It is direct from $f_{150(n),a-b}(x) = f_{150(n),0-0}(x) + a0^{n-2}b$ and $f_{150(n),a-*}(x) = f_{150(n),0-*}(x) + a0^{n-1}$. (3,4) This can be shown in the same way as the proof of Corollary 8.2. $\square$

Corollary 8.4 (a) *$CA{-}150_{a-b}(n)$ is reversible iff $n \neq 2$ (mod3).*

(b) *$CA{-}150_{a-*}(n)$ is reversible iff $n \neq 1$ (mod3).*

9 $CA{-}\{166, 180, 154, 210, 89, 75, 101, 45\}(n)$

It is obvious that $f_{166}(abc) = (a+1)b + c$, $f_{180}(abc) = a + b(c+1)$, $f_{154}(abc) = a(b+1) + c$, $f_{210}(abc) = a + (b+1)c$, $f_{89}(abc) = (a+1)b + c + 1$, $f_{75}(abc) = a + b(c+1) + 1$, $f_{101}(abc) = a(b+1) + c + 1$, $f_{45}(abc) = a + (b+1)c + 1$ for all triples $abc \in Q^3$, $f_{166}^{-} = f_{89}$, $[166, 180, 154, 210]$ and $[89, 75, 101, 45]$. Hence by Corollary 3.2 and Lemma 3.3 the reversibilities of cellular automata $CA{-}\{166, 180, 154, 210, 89, 75, 101, 45\}(n)$ are equivalent and so we will inspect only $CA{-}166(n)$.
We now use the following notation:

$$x_1^{(1)} x_2^{(1)} \cdots x_n^{(1)} = f_{166(n),*}(x_1 x_2 \cdots x_n),$$

$$x_1^{(k+1)} x_2^{(k+1)} \cdots x_n^{(k+1)} = f_{166(n),*}(x_1^{(k)} x_2^{(k)} \cdots x_n^{(k)})$$

for each configuration $x_1 x_2 \cdots x_n \in Q^n$. In other words,

$$x_1^{(k)} x_2^{(k)} \cdots x_n^{(k)} = (f_{166(n),*})^k (x_1 x_2 \cdots x_n),$$

where $(f_{166(n),*})^k$ is k-th composition of $f_{166(n),*}$. Also a configuration $x_1 x_2 \cdots x_n$ in $CA{-}166_*(n)$ is extended to an infinite configuration $(x_m)_{m \in \mathbb{Z}}$ such that $x_m = x_{m'}$ if $m = m'$ (mod n).

Lemma 9.1 *In $CA{-}166_*(n)$ an identity*

$$x_m^{(2^k)} = (x_{m-2^k} + 1)\Pi_{j=1}^{2^k} x_{m-2^k+2j-1} + x_{m+2^k}$$

holds for all natural numbers m and k.

Proof. (i) In the case of $k = 0$ an identity

$$x_m^{(1)} = (x_{m-1} + 1)x_m + x_{m+1}$$

holds, since $f_{166}(abc) = (a+1)b + c$.
(ii) Set $\delta = f_{166(n),*}$. Assume that the identity holds for a natural number k. Note that

$$\delta^{2^{k+1}}(x) = (\delta^{2^k} \delta^{2^k})(x) = \delta^{2^k}(x_1^{(2^k)} x_2^{(2^k)} \cdots x_n^{(2^k)}).$$

Hence by using the induction hypothesis twice we have

$$
\begin{aligned}
x_m^{(2^{k+1})} &= (x_{m-2^k}^{(2^k)}+1)\Pi_{j=1}^{2^k} x_{m-2^k+2j-1}^{(2^k)} + x_{m+2^k}^{(2^k)} \\
&= \{(x_{m-2^{k+1}}+1)\Pi_{j=1}^{2^k} x_{m-2^{k+1}+2j-1} + x_m + 1\} \\
&\quad \Pi_{j=1}^{2^k}\{(x_{m-2^{k+1}+2j-1}+1)\Pi_{i=1}^{2^k} x_{m-2^{k+1}+2j+2i-2} + x_{m+2j-1}\} \\
&\quad +(x_m+1)\Pi_{j=1}^{2^k} x_{m+2j-1} + x_{m+2^{k+1}} \\
&\quad \{\ m-2^{k+1}+2j+2i-2 = m \text{ for } i = 2^k - j + 1\ \} \\
&= \{(x_{m-2^{k+1}}+1)\Pi_{j=1}^{2^k} x_{m-2^{k+1}+2j-1} + x_m + 1\}\Pi_{j=1}^{2^k} x_{m+2j-1} \\
&\quad +(x_m+1)\Pi_{j=1}^{2^k} x_{m+2j-1} + x_{m+2^{k+1}} \\
&= (x_{m-2^{k+1}}+1)\Pi_{j=1}^{2^{k+1}} x_{m-2^{k+1}+2j-1} + x_{m+2^{k+1}},
\end{aligned}
$$

which completes the proof. □

Corollary 9.2 *CA–$166_*(n)$ is reversible iff $n = 1$ (mod 2)*

Proof. It is trivial that $f_{166(1),*}(x_1) = x_1$ and so $f_{166(1),*}$ is bijective. Next we will see that every transition function $f_{166(2n-1),*} : Q^{2n-1} \to Q^{2n-1}$ of CA–$166_*(2n-1)$ is bijective for all integers $n \geq 2$. Take a unique integer k such that $2^k < 2n-1 < 2^{k+1}$. By the virtue of the last lemma 9.1 the m-th state of $(f_{166(2n-1),*})^{2^k}(x)$ is given by

$$x_m^{(2^k)} = (x_{m-2^k}+1)\Pi_{j=1}^{2^k} x_{m-2^k+2j-1} + x_{m+2^k}$$

Set $j = n$. (Remark $2 \leq n \leq 2^k$.) Then $m - 2^k + 2j - 1 = m - 2^k \pmod{2n-1}$ and so $(x_{m-2^k}+1)x_{m-2^k+2j-1} = (x_{m-2^k}+1)x_{m-2^k} = 0$. Hence we have

$$x_m^{(2^k)} = x_{m+2^k},$$

which proves the bijectivity of $f_{166(2n-1),*}$. Finally we see that every transition function $f_{166(2n),*}$ is not injective. It follows at once from

$$f_{166(2n),*}((01)^n) = f_{166(2n),*}((10)^n) = 0^{2n}.$$

This completes the proof. □

Lemma 9.3 (a) *CA–$166_{\{1-b,0-*,*-b\}}(n)$ are not reversible for all positive integers n.*

(b) *CA–$166_{\{0-b,1-*,*-*\}}(n)$ are not reversible for any positive integers $n \geq 2$.*

Proof. It is direct from the following equations;

- $f_{166(n),0-b}(110^{n-2}) = f_{166(n),0-b}(0^n)$ for $n \geq 2$
- $f_{166(1),0-*}(x_1) = 0$

- $f_{166(2),0-*}(10) = f_{166(2),0-*}(01)$
- $f_{166(n),0-*}(110^{n-2}) = f_{166(n),0-*}(0^n)$ for $n \geq 3$
- $f_{166(1),1-b}(x_1) = b$
- $f_{166(n),\{1-b,1-*\}}(10^{n-1}) = f_{166(n),\{1-b,1-*\}}(0^n)$ for $n \geq 2$
- $f_{166(n),*-b}(10^{n-1}) = f_{166(n),*-b}(0^n)$
- $f_{166(n),*-*}(10^{n-1}) = f_{166(n),*-*}(0^n)$ for $n \geq 2$

□

10 Conclusion

We have proved that several 1d CA with finite cell array, including cyclic CA simulated in [9], are reversible. According to computer simulation we can simply observe that $CA - R(n)$ except for those which are verified in the paper are not reversible. Wolfram showed that for 1d CA with infinite cell array there exist the only six reversible CA with trivial triplet local rules. However the paper presented some nontrivial 1d CA with finite cell array. The reversible CA dealt with in this paper are special type of QCA. Our future work is to investigate how these reversible $CA - R(n)$ are extended to generalised PQCA introduced by [9].

References

[1] S. Wolfram, Theory and applications of cellular automata, World Scientific, Singapore (1986).

[2] K. Morita and M. Harao, Computation universality of one-dimensional reversible (injective) cellular automata, Transactions of the IEICE, Vol. E 72 (1989) 758-762.

[3] E. Goles and S. Martinez, Neural and automata networks - dynamical behavior and applications -, Kluwer Academic Publishers, Dordrecht (1990).

[4] J. Watrous, On one-dimensional quantum cellular automata, Proceedings on the 36th Annual Symposium on Foundations of Computer Science (1995) 528-537.

[5] H.-Y. Lee and Y. Kawahara, Transition diagrams of finite cellular automata. Bull. Inform. Cybernet. **28** (1996) 47-69.

[6] S. Inokuchi et al., Computational analysis of cellular automata with triplet transition rule. Research Reports on Information Science and Electrical Engineering of Kyushu University **1**(1) (1996) 79-84 (in Japanese).

[7] R.A. Dow: Additive Cellular Automata and Global Injectivity, Physica D 110 (1997) 67-91.

[8] S. Wolfram, A New Kind of Science, Wolfram Media, Inc. (2002) 435-457, 1017-1021.

[9] S. Inokuchi and Y. Mizoguchi, Generalized Partitioned Quantum Cellular Automata and Quantization of Classical CA, Int. Journ. of Unconventional Computing, Vol. 1 (2005) 149-160.